HW2

Andrew Rosen

October 6, 2013

1 Question 1

1.1 Part a

$$P = (C \boxplus \bar{K_1}) \oplus K_0$$

where $\bar{K_1}$ is the complement of K_1.

1.2 Part b

Let our plaintext messages be P_a, P_b and their corresponding ciphertexts be C_a, C_b. We know that

$$C_n = (P_n \oplus K_0) \boxplus K_1$$

We can define K_0 in terms of C_a, P_a, and K_1 by rearranging the variables.

$$(P_n \oplus K_0) \boxplus K_1 = C_n$$

$$P_a \oplus K_n = C_a \boxplus \bar{K_n}$$

$$K_0 = (C_n \boxplus \bar{K_1}) \oplus P_n$$

Which means you can't solve it without solving $\bar{K_1}$ or K_1.

$$(C_a \boxplus \bar{K_1}) \oplus P_a = (C_b \boxplus \bar{K_1}) \oplus P_b$$

$$(C_a \boxplus \bar{K_1}) \oplus P_a \oplus P_b = C_b \boxplus \bar{K_1}$$

$$\big((C_a \boxplus \bar{K_1}) \oplus P_a \oplus P_b\big) \boxplus C_b = \bar{K_1}$$

The solution is intractably self-referential, as $\oplus$ is not distributive. There is no easy solution for K_0 or K_1.

2 Question 2

I will solve this problem for the general case. Let me denote the encryption of message m as $E(m)$, since the key is not relevent here. The defined encryption scheme being linear means

$$E(m_a) \oplus E(m_b) = E(m_a \oplus m_b)$$

This also implies that a message made of all zeroes will be encrypted to a message of all zeroes.

Now, let each input m_i and corresponding output $E(m_i)$ be l bits long. Choose l ciphertexts $E(m_i)$ such that

$$\begin{aligned}
E(m_1) &= 1000\ldots \\
E(m_2) &= 0100\ldots \\
E(m_3) &= 0010\ldots \\
&\ldots \\
E(m_{l-1}) &= \ldots 0010 \\
E(m_l) &= \ldots 0001
\end{aligned}$$

I denote this set $\mathscr{E}$. If I know the corresponding plaintexts $\{m_1, m_2, \ldots m_l\}$, I can decipher any message using the linear property of E. Let $E(m_k)$ be an intercepted message. $E(m_k$ can be described by XORing a unique subset of $\mathscr{E}$. Now becuase of the linear property of E, I can retreive m_k by XORing the m's that correspond to the aforementioned unique subset.

For example, let

$$E(m_k) = E(m_1) \oplus E(m_{17}) \oplus E(m_{42})$$

We can retrieve m_k via

$$m_k = m_1 \oplus m_{17} \oplus m_{42}$$

3 Question 3

3.1 i

Since Bob already knows k and he knows the length of v, $(v||c)$ is effectively (v, c), yeilding:

$$m = \text{RC4}(v||k) \oplus c$$

.

3.2 ii

If $v_i = v_j$, then $(v_i||k) = (v_j||k)$, meaning the same input to RC4 would have been used.

4 Question 4

All RSA operations with a given key occur in the same mod space. For brevity, assume that every mathematical operation below has an unwritten mod n as a component.

This question can be solved via expansion. We have been given B_1 and B_2, as well as C_1, as well as key$\{e, n\}$. Let us solve for C_2 such that $RSAH(C_1, C_2) = RSAH(B_1, B_2)$.

$$RSAH(C_1, C_2) = RSA(RSA(B_1) \oplus B_2) = RSA(B_1^e \oplus B_2)$$

$$RSA(RSA(C_1) \oplus C_2) = RSA(B_1^e \oplus B_2)$$

$$(C_1^e \oplus C_2)^e = (B_1^e \oplus B_2)^e$$

$$C_1^e \oplus C_2 = B_1^e \oplus B_2$$

$$C_2 = C_1^e \oplus (B_1^e \oplus B_2)$$

Thus we can always choose a C_2 s.t. $RSAH(C_1, C_2) = RSAH(B_1, B_2)$, and $RSAH$ does not satisfy weak collision resistance ■